NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

COUNTERFEIT ELECTRONIC PARTS CONTROLS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

By: Joseph M. Russell

June 2015

Advisors: Brad Naegle
Michael Boudreau

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
June 2015

3. REPORT TYPE AND DATES COVERED
Joint Applied Project

4. TITLE AND SUBTITLE
COUNTERFEIT ELECTRONIC PARTS CONTROLS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

5. FUNDING NUMBERS

6. AUTHOR(S) Joseph M. Russell

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Counterfeit electronic parts in the Department of Defense (DOD) supply chain undermine the operational readiness and performance of weapons systems, provide a competitive edge to adversaries, and put warfighters at risk. Consumer demand for products containing integrated circuits has risen dramatically. Electronics manufacturers leverage overseas production to reduce cost. The loss of the domestic semiconductor industry and a variety of DOD acquisition policies contributed to an environment that introduces risk of foreign manufactured components of unverifiable pedigree into many DOD systems. Current policy and statutory controls are inadequate to stem the growth of counterfeit and nonconforming parts in the DOD supply chain. This Joint Applied Project considers the history and scope of the counterfeit parts issue and its contributing factors, and proposes a tiered solution to more effectively ensure the safety, quality, and specification conformance of integrated circuit components.

14. SUBJECT TERMS Counterfeit Parts, Integrated Circuits, Supply Chain Risk Management

15. NUMBER OF PAGES
57

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COUNTERFEIT ELECTRONIC PARTS CONTROLS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

Joseph M. Russell

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2015

Author: Joseph M. Russell

Approved by: Brad Naegle

Michael Boudreau

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

COUNTERFEIT ELECTRONIC PARTS CONTROLS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

ABSTRACT

Counterfeit electronic parts in the Department of Defense (DOD) supply chain undermine the operational readiness and performance of weapons systems, provide a competitive edge to adversaries, and put warfighters at risk. Consumer demand for products containing integrated circuits has risen dramatically. Electronics manufacturers leverage overseas production to reduce cost. The loss of the domestic semiconductor industry and a variety of DOD acquisition policies contributed to an environment that introduces risk of foreign manufactured components of unverifiable pedigree into many DOD systems. Current policy and statutory controls are inadequate to stem the growth of counterfeit and nonconforming parts in the DOD supply chain. This Joint Applied Project considers the history and scope of the counterfeit parts issue and its contributing factors, and proposes a tiered solution to more effectively ensure the safety, quality, and specification conformance of integrated circuit components.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

BIS	Bureau of Industry and Statistics
CAS	Cost Accounting Standard
COTS	Commercial-Off-The-Shelf
CDD	Capabilities Development Document
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DMEA	Defense Microelectronics Activity
DOD	Department of Defense
DSB	Defense Science Board
GAO	Government Accountability Office
GIDEP	Government and Industry Data Exchange Program
IEEE	Institute of Electrical and Electronics Engineers
MIL-SPEC	Military Specification
MIL-STD	Military Standard
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
OCM	Original Component Manufacturer
OEM	Original Equipment Manufacturer
RFID	Radio Frequency Identification
SASC	Senate Armed Services Committee
SECDEF	Secretary of Defense
SWPaC	Space, Weight, Power, and Cooling
TR	Technology Refresh
USD AT&L	Under Secretary of Defense for Acquisition, Technology, Logistics

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM DESCRIPTION

Statutory measures designed to stem the flow of counterfeit electronic parts into the Department of Defense (DOD) supply chain are not effective at curbing the threat. Vendors are behind the threat curve. Control measures are designed to identify counterfeit parts after they have reached the customer, and are inadequate at addressing the core issues behind the problem. A joint contractor/government approach is required, in all phases of the acquisitions life cycle, in order to adequately address the problem.

B. BACKGROUND INFORMATION

Counterfeit electronics in the DOD supply chain undermine the operational readiness and performance of weapons systems, degrade the competitive edge that our weapons otherwise provide, and put warfighters at risk.

Consumer demand for products that use integrated circuits has risen steadily since their invention; with the rise in demand, comes vendor pressure to maintain supply. Electronics manufacturers understood this in the early days of the industry, and shipped much of the production work overseas in order to capitalize on reduced labor costs. According to Rochester Electronics (2011), the foreign manufacture of integrated circuits opened the door to a risk that was not adequately mitigated upon its first identification, and is estimated to cost the American economy over $5 billion per year. It is also estimated that more than 2% of the total available semiconductor market is composed of counterfeit parts (Rochester Electronics, 2011, p. 2).

The issue of counterfeit parts has now become a global concern in both the public and private sectors. The problem is especially serious for the DOD; with parts being manufactured in countries that have a tense relationship with the United States, while countries that are considered friendly to the United States act as infiltration points to United States markets (Rochester Electronics, 2011, p. 2). The United States bears much of the responsibility for perpetuating this problem through acquisitions policies that favor independent parts brokers, an ever-increasing service life for systems that require replacement electronic parts, and a life cycle management plan that does not adequately account for disposal of nonconforming parts or retired systems (H.R. 1540, 2012).

The DOD identified counterfeit parts risks to the supply chain as early as 1986, and has made attempts since that time to bound the problem of counterfeit parts (U.S. Department of Defense, 1986). There has been some success at the identification of the problem itself, but the actual numbers of counterfeit parts that are currently embedded in military systems is unknown, as is the actual number of counterfeit parts that are in a warehouse pending assembly into a military system.

The latest attempt to combat the problem is in the form of congressional policy that directly addresses the issue at the prime contractor level. The 2012 National Defense Authorization Act Section 818 (H.R. 1540, 2012), and the subsequent Secretary of Defense memorandum (Kendall, 2012), provide the most comprehensive guidance to date, with specific statutory measures aimed at contractors who supply microcircuits to the DOD. These controls, however, fall short of the actions that are required to adequately combat the problem.

This research intends to show that counterfeit electronics are a problem that cannot be solved by pushing the full identification and mitigation responsibility on the contractor. Rather, these parts need to be caught before they enter the contractor facility or DOD warehouse. The analysis presented will clearly demonstrate that there needs to be a focused, joint government and contractor effort to identify solutions that benefit both. The DOD needs to take active steps to combat this epidemic before inexpensive, nonconforming parts that accidentally find their way into United States combat systems are replaced with parts that are specifically targeted and designed to infiltrate and undermine the military‘s ability to defend.

C. PROJECT DESCRIPTION AND APPROACH

This project examines the history and scope of the counterfeit parts problem, assesses the adequacy of current policy and statutory controls, and proposes the development of a tiered strategy to address the issue.

II. SCOPE OF THE PROBLEM

A. HISTORY

Counterfeit parts have been an issue since the early days of the integrated circuit. The United States government has not addressed the problem until recently (U.S. Department of Defense, 1986), partly because the problem has not been adequately scoped.

The early days of digital computing were relatively simple, consisting of large machines weighing several tons computing through the use of vacuum tubes. The computing took place when the tubes would amplify current and pass electrical signals from one part of the program to another. According to Nobelprize.org, the Nobel Prize official website, the first digital computer weighed 30 tons and used 18,000 vacuum tubes (Nobel Prize, 2014). An example of an early, typical room size computer is shown in Figure 1.

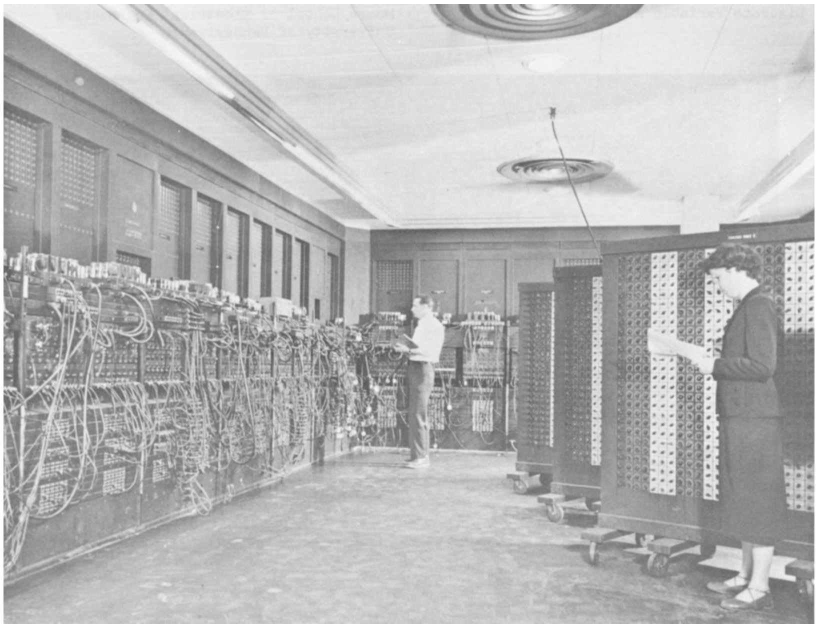


Figure 1. Early Vacuum Tube Computer. An early computer that incorporated the use of vacuum tubes is shown. Large ceiling air ducts were required to keep the vacuum tubes of this unit cool (from Historic Computer Images, 2013).

The invention of the transistor in 1947 revolutionized the world of computing. Transistors function the same way as vacuum tubes, but are much smaller, less prone to burning out, and provided engineers a new way to think about computing design (Nobel Prize, 2014). Without the anchor of the vacuum tubes, engineers began to conceive of advanced processing machines, but there was an existing problem with the circuits of the day (Nobel Prize, 2014). Each circuit required hand assembly and soldering of each individual component in order to form the necessary connections to complete the circuit (Nobel Prize, 2014). A single circuit was labor intensive and a simple mistake would cause the whole circuit to fail (Nobel Prize, 2014).

In 1958, an engineer working at Texas Instruments had the idea to place the whole circuit on a single piece of semi-conductive material; with this idea, the need for individual soldering of connections and long production times was completely negated (Nobel Prize, 2014). All the transistors, resistors, capacitors, and diodes which form a chip, were integrated into a single block, which was reproducible through an automated manufacturing process (Nobel Prize, 2014).

The invention of the integrated circuit brought about a transformation in computer hardware development, manufacturing, and associated software design. The ability to pack the same computing power that previously required 18,000 vacuum tubes onto a small microchip was a milestone for hardware development, but the fact that it could be mass produced and used interchangeably meant that computing was accessible to the masses (Nobel Prize, 2014). Stages in the evolution of the modern microprocessor are depicted in Figure 2.

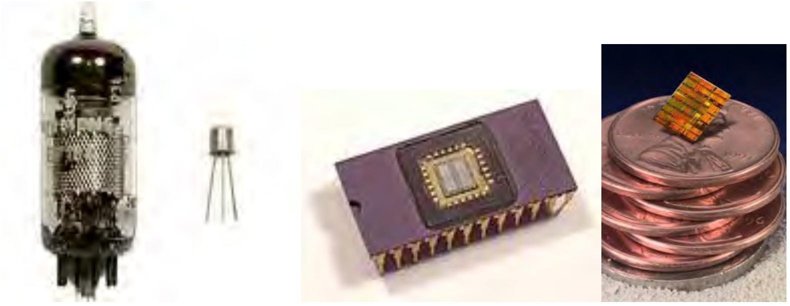


Figure 2. Evolution of the Microprocessor. Left: Vacuum tube pictured next to an early transistor (from Nobel Prize, 2014). Center: Representation of a common transistor (from Nobel Prize, 2014). Right: The scale of this microprocessor is evident as it sits on a stack of pennies (from How Microprocessors Work, 2013).

Engineers quickly realized the possibilities if these microchips were placed into weapons systems. The creation of ―smart-weapons” was underway, with each system having its own autonomous decision making logic on board. DOD much preferred smart weapons for the functionality they added in the form of precision guidance systems, diagnostic outputs, and reduced loss of non-combatant lives. Strictly from a size perspective, the Space, Weight, Power, and Cooling (SWPaC) requirements for these new microchips and the systems into which they were incorporated greatly decreased the footprint of the platforms on which these were installed. The reduced SWPaC footprint meant that faster systems, and more of them, could be placed where one computer was previously housed. An example of a large shipboard computer with substantial SWPaC requirements is shown in Figure 3.

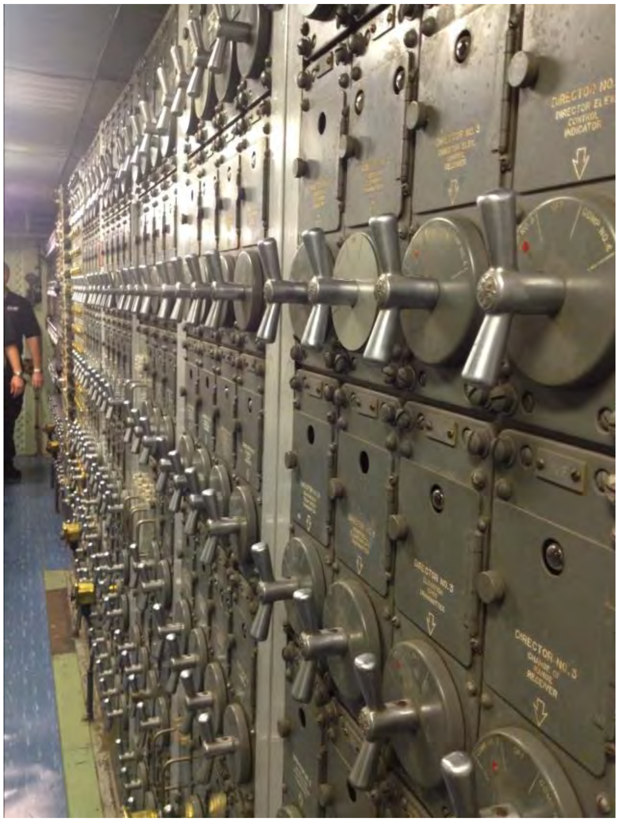


Figure 3. USS Missouri Fire Control Computer. The USS Missouri was commissioned in 1945 and was retired from service in 1992. This fire control computer was designed in 1941. The same type of computer for a modern-day ARLEIGH BURKE class Guided Missile Destroyer takes up a fraction of a commercial blade server rack (from Rumberg, 2013).

B. GOVERNMENT/INDUSTRY DATA EXCHANGE PROGRAM (GIDEP)

As early as 1980, there were indications that some of the parts used in operational weapons systems were not performing to their required standard; these parts were referred to as ―non-conforming” (U.S. Department of Defense, 1986). The existence of non-conforming parts and the implication that the reliability of the weapons system would not function according to the specifications caused concern, and prompted the development of the 1986 MIL-STD-1556B, which set guidelines for contractor participation in the Government/Industry Data Exchange Program (GIDEP). The purpose of the GIDEP was to provide

> a cooperative data interchange among Government and industry participants seeking to reduce or eliminate expenditures of time and money by making maximum use of existing knowledge. ...Information contained within the GIDEP storage and retrieval system includes environmental test reports and procedures, reliability specifications, failure analysis data, failure rate data, calibration procedures, and other technical information related to the application, reliability, quality assurance, and testing of parts and related materials. (U.S. Department of Defense, 1986, p. iii)

Though the problem of counterfeit parts had not been identified or specifically addressed at this point, the GIDEP was the first step towards quantifying the problem of non-conforming parts within the DOD supply chain. In section 5.3.2 of MIL-STD-1556B, it is stated that contractor participation is voluntary unless contractually stipulated (U.S. Department of Defense, 1986, p. 7).

There was an obvious reluctance on the part of the contractor to voluntarily report non-conforming parts for fear that their quality control practices or suppliers would be brought into question. There was no monitoring program in place to ensure contractor participation, and there was no monitoring program in place to ensure their sub-contractors participated. Additionally, there was no quality assurance standard that had to be met.

Ten years after its inception, MIL-STD-1556B was formally cancelled as part of DOD Acquisition reforms, and has not been replaced. The 1996 cancellation notice did provide details as to the location of the GIDEP operations manual and suggested contractual language for the future use of the system, but the formal guidelines that governed the contractual use of GIDEP had been suspended (U.S. Department of Defense, 1996, p. 1). Though the 1986 standard fell short of accurately quantifying the issue of counterfeit parts, it did lay the groundwork for cross-agency collaboration to combat a problem that was largely not understood. As of 2015, participation in GIDEP by industry members is entirely voluntary, and represents ~~a~~ cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information" (GIDEP Home Page, 2015, para. 1).

C. POST-MIL-STD-1556B POLICY GAP

Although no longer documented in a formal MIL-STD, DOD had taken notice of the importance of microelectronics, as well as the possible vulnerabilities that were introduced as a result of the extensive use and dependence upon them. The Defense Science Board (DSB) issued a 1992 report titled *Microelectronics Research Facilities*. In that report, the DSB reached a conclusion, as reported to the director for defense research and engineering, that: ―DOD needs a strong microelectronic science and technology program which encourages diversity and innovation in all phases from research through system development and support. The objective of this program should be to assure Defense Department access to and insertion of microelectronics technology to support its needs" (Defense Science Board, 1992, p. 5).

The DSB had identified the need for the United States to remain the leader in technological development, and pinpointed the ―pervasive, enabling" effects of microelectronics on DOD systems. The DSB report went a step further and called upon DOD to create a single research facility, combining Tri-Service approaches to the development and incorporation of microelectronics technology. Their fear in 1992 was the increasing global demand for microelectronics, and the threat that the United States would no longer be at the forefront of the technological curve. The DSB suggested high level DOD oversight that would ensure industry would continue to provide reliable access to critical technologies, and provide ―smart-buyer" capabilities to keep the United States at the forefront of technological proficiencies (Defense Science Board, 1992, p. 7).

The major threat to the United States was noted as early as 2005, when the DSB issued a report, *High Performance Microchip Supply*. In this report, they identified the growth of global demand for integrated circuits and discrete electronic parts had risen, which put pressure on industry to reduce labor costs and to spread production risks across a broader area (Defense Science Board, 2005). In order to respond to this need, chip makers, who were predominately located in the United States, moved their production operations overseas, as noted by the National Academy of Engineering:

> In the semiconductor industry, some steps (e.g., assembly, packaging, and testing) in the manufacturing process have long been globalized. In recent

> years, more sophisticated steps, such as wafer fabrication, have followed suit. Off shoring of semiconductor design is also increasing rapidly, in fact, 18 of the top 20 U.S.-based companies have opened design centers in India, nine of them since 2004. (National Academy of Engineering, Committee on the Offshoring of Engineering, 2008, p. 34)

In 2005, the DSB again called upon the DOD to protect the technical leadership of the United States in order to

> ensure that the United States maintains reliable access to the full spectrum of microelectronics components, from commodity and legacy, to state-of-the-art parts, and application-specific Integrated Circuits special technologies. These activities must provide assurance that each component‘s trustworthiness (confidentiality, integrity, and availability) is consistent with that component‘s military application. (Defense Science Board, 2005, p. 52)

More importantly, they took note of the need for long term planning and focus in the acquisition of critical technologies that require the use of microelectronics: ―DOD needs a focused, tailored acquisition plan, driven by a long-term vision of its semiconductor needs, to establish the basis, policy and operating guidelines for DOD-enabled access to trusted foundry services by the defense department, its contractors, and others" (Defense Science Board, 2005, p. 56).

Despite all the intra-governmental warnings and indications of possible systemic vulnerabilities to the microchip supply line, the issue first garnered national attention in 2008 when Business Week published an article titled *Dangerous Fakes – How Counterfeit, Defective Computer Components from China are Getting into U.S. Warplanes and Ships* (Grow, Tschang, Edwards, & Burnsed, 2008). The article identifies major flaws in DOD acquisitions and specifically cites China as a source of the problem and provider of non-conforming parts.

D. SCOPING THE PROBLEM

The problem of counterfeits had been publicly identified and acknowledged, but the full scope was not understood until the Department of Commerce, Bureau of Industry and Security (BIS) published their Defense Industrial Base Assessment for Counterfeit Electronics in 2010 (U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010). This report was the first attempt to turn the problem of counterfeit parts from anecdotal information to definitive facts.

Spanning a four year period, BIS reported that nearly 40% of survey respondents (inclusive of manufacturers, distributors, assemblers, and contractors) had encountered counterfeit parts. Additionally, the detection rate for counterfeits had risen from 3,868 in 2005 to 9,365 in 2008. Of those parts that are most counterfeited, microcircuits and their components represent the highest frequency of occurrence. One of the primary reasons for this rise, as noted by BIS, is quite simply that weapons systems life cycles are extending well beyond their initial service life, which makes genuine replacement parts increasingly more difficult to acquire. The counterfeiting of low-cost and comparatively low tech components both, makes the practice more accessible in developing nations and makes the modified parts more commonplace in the supply chain (U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010). As shown in Figure 4, the value of the most commonly counterfeited parts is less than $10.00 USD.

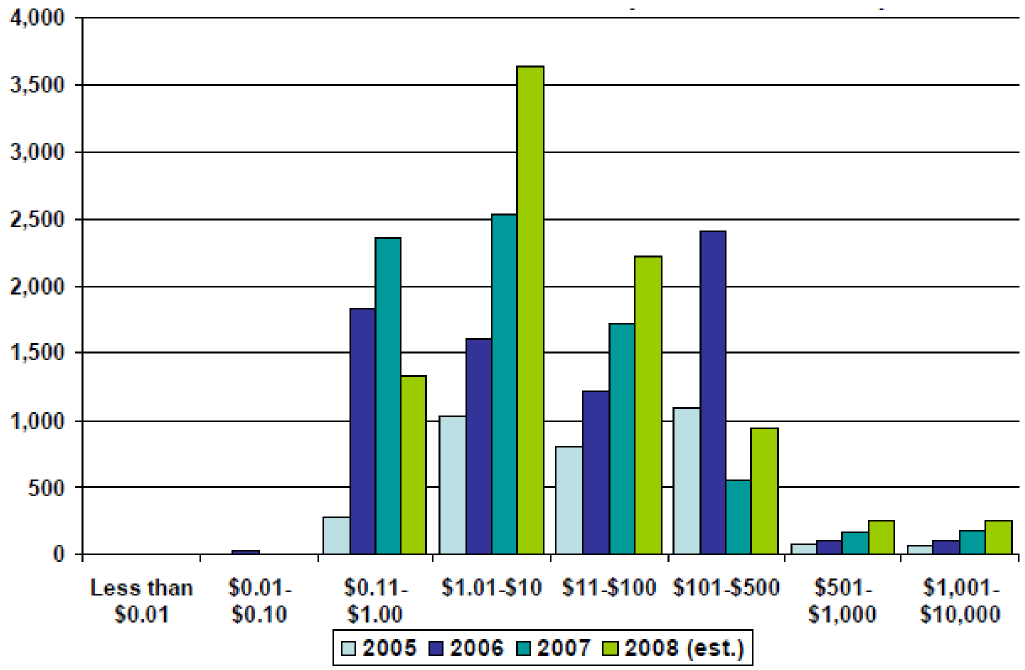


Figure 4. Counterfeit Incidents by Product Resale Value, OCMs (2005-2008). This graph shows the average value of individual counterfeited parts during 2005–2008. Most counterfeited parts cost $10.00 USD or less. These are small components that are incorporated in the subsystem and system levels of products, and often go unnoticed (from U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010, p. 12).

The Original Component Manufacturer (OCM) is the manufacturer of discrete electronic parts, and primarily supplies those parts to Original Equipment Manufacturers (OEM), prime and subcontractors, and entities of the United States government that incorporate them into systems. As noted by the BIS, OCMs and OEMs sell their products to authorized distributors, independent distributors, and parts brokers, which in turn sell those products to a wide variety of customers. Distributors act as middle-men, finding the ~~–o~~ut of production" parts for their customers, but there are many different flavors of distributor:

> Authorized distributors are companies that have exclusive rights with an OCM or OEM to market, store, and ship OCM/OEM Products, subject to legal conditions set by the manufacturers. Conversely, independent distributors and brokers sell parts acquired from various entities without

> an exclusive OCM/OEM agreement to do so. Independent distributors tend to maintain inventories and have controlled environments for parts storage. Brokers tend to be smaller firms and normally do not have inventory or controlled environments. (U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010, p. 39)

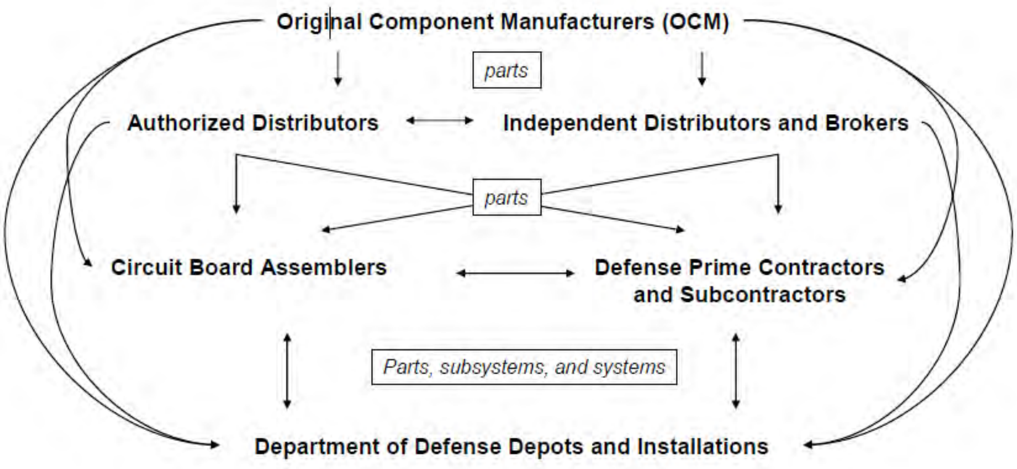

Original Component Manufacturers (OCM)
parts
Authorized Distributors
Independent Distributors and Brokers
parts
Circuit Board Assemblers
Defense Prime Contractors and Subcontractors
Parts, subsystems, and systems
Department of Defense Depots and Installations

Figure 5. United States Defense Electronic Parts Supply Chain. This depicts the basic flow of electronic parts between OCMs, distributors, assemblers, and contractors prior to delivery to DOD Components (from U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010, p. 4).

As there is no inventory maintained by independent parts brokers, there is a risk that parts will get shipped directly from source-to-depot, without any verification checks or independent testing. An example of the dangers surrounding independent brokers is highlighted in *Bloomberg Business*:

> She (Hakimuddin) began brokering military chips four years ago, after friends told her about the expanding trade. Since 2004 she has won Pentagon contracts worth a total of $2.7 million, records show. The military has acquired microchips and other parts from IT Enterprise for use in radar on the aircraft carrier USS Ronald Reagan and the antisubmarine combat system of Spruance-class destroyers.
>
> Hakimuddin says she knows little about the parts she has bought and sold. She started her business by signing up on the Internet for a Government supplier code. After the Defense Dept. approved her application, with no

> inspection, she began scanning online military procurement requests. She plugged part codes into Google and found Websites offering low prices. Then she ordered parts and had them shipped directly to military depots. ―I wouldn‘t know what [the parts] were before I‘d order them,” she says, standing near her front door. ―I didn‘t even know what the parts were for.” (Grow, Tschang, Edwards, & Burnsed, 2008)

There was no verification of MIL-SPEC conformance, there was no pedigree paperwork associated with this transaction, and there was no independent parts inspection. It is highly likely that those parts, destined for the radar of the USS Ronald Reagan, shipped directly from China to the radar assembly plant. Once received in the assembly plant, the manager likely assumed the parts were all conforming, and likely put them directly into the production line (Grow, Tschang, Edwards, & Burnsed, 2008).

While the BIS survey helped the United States to gain some understanding as to the possible amount of counterfeit parts that are likely to be in the supply line, the Senate Armed Services Committee (SASC) provided the details as to their means of infiltration in their 2012 report titled *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (U.S. Senate Committe on Armed Services, 2012).

The SASC identified the United Kingdom and Canada as major infiltration points for counterfeit material into the United States, with China as the primary origination point of manufacture for counterfeit electronics. The report further noted that the Chinese counterfeiting market is deep-rooted, enjoys strong support from the people of China, and is in no danger of shut-down by the Chinese government. According to the SASC, the raw materials that are used by Chinese counterfeiters are obtained through recycled electronic waste that mostly originates in the United States (U.S. Senate Committe on Armed Services, 2012).

In theory, the recycling of electronic waste is an ethical environmental decision. An older, functional integrated circuit that was formerly used in an obsolete computer can be turned around and used for a lower level application that does not have the same performance requirements (calculators, home appliances); however, some scrap recycling companies realize profits when they send their raw materials to Hong Kong for disposal (U.S. Senate Committe on Armed Services, 2012). From there, electronic waste is put on trucks and shipped into mainland China, where the electronic devices are taken apart for scrap, sorted, cleaned, re-labeled, and in most cases, re-sold as new products to independent brokers, which eventually make their way back to the United States (U.S. Senate Committe on Armed Services, 2012).

The SASC survey included testimony from industry representatives who traveled to China to witness the counterfeiting markets first hand.

> While there, I witnessed e-scrap piled outside of buildings throughout large areas of the town, throughout the outskirts of the town, used electronic parts being washed in a river, and laid on the riverbank to dry, Nylon sacks with harvested components being dumped onto sidewalks and sorted by women and children, laid out there for the monsoon rains of July to wash them naturally, cardboard and plastic bins filled with expensive brand name components and harvested from scrap printed circuit boards ready for processing. (U.S. Senate Committe on Armed Services, 2012, p. 6)

E. TECHNIQUES

Counterfeiting is not relegated to villagers on the sides of a riverbank. According to SASC Testimony, in the Guangdong Province, there are entire factories dedicated to the counterfeiting industry, some of which employ 10,000 – 15,000 people. In these factories, circuit boards are processed and made to look original through a variety of means. The pins on the circuit are straightened, and labels are changed to indicate a new or higher performing part numbers (U.S. Senate Committe on Armed Services, 2012). The most common form of counterfeiting is a process called ―Blacktopping,” where the old part is given a fresh coat of paint that looks indistinguishable from the original paint to the average purchaser (Villasenor & Tehranipoor, 2013).

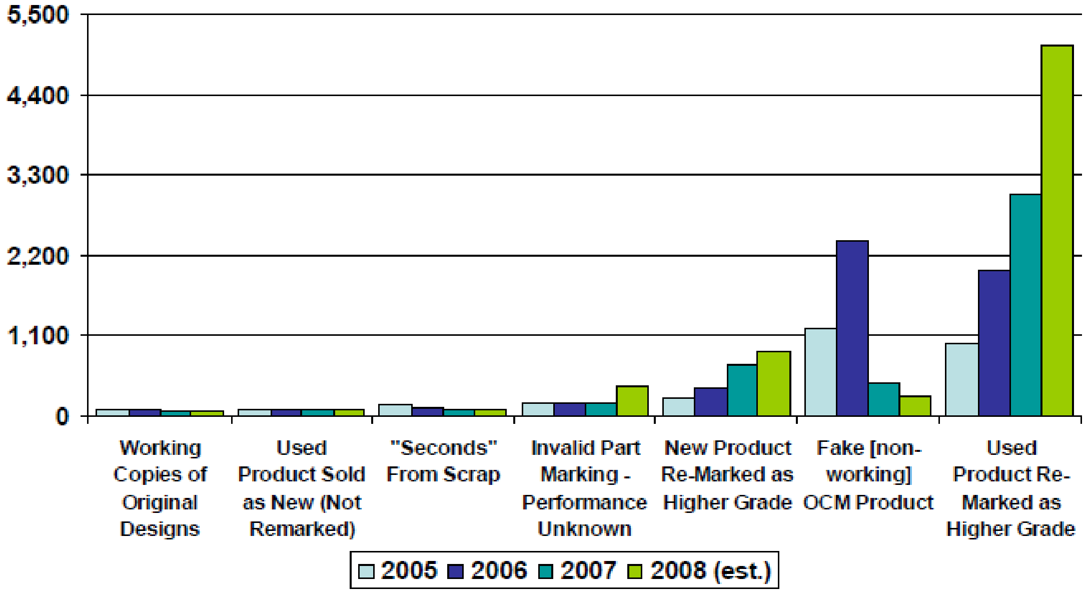


Figure 6. Counterfeit Microcircuit Incidents by Type of Problem (2005-2008). This graph shows the types of counterfeiting that are prevalent for microcircuits. Note the sharp increase in products that are marked as higher grade, and the relatively low number of ―seconds" from scrap. This is attributable to the increasing sophistication of the counterfeiting industry in China, and the ease with which relabeling occurs (from U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, 2010, p. 16).

The counterfeiting market in China is sophisticated, and has shown an ability to adapt and change as needed to avoid detection. For example, a simple test to see if a chip has been blacktopped is to run an acetone soaked swab over the top of it to see if paint comes off. This worked until 2009 when a company discovered that counterfeiters had developed a paint that more closely resembled the chemistry of the original paint, thereby making the swab test invalid (Villasenor & Tehranipoor, 2013).

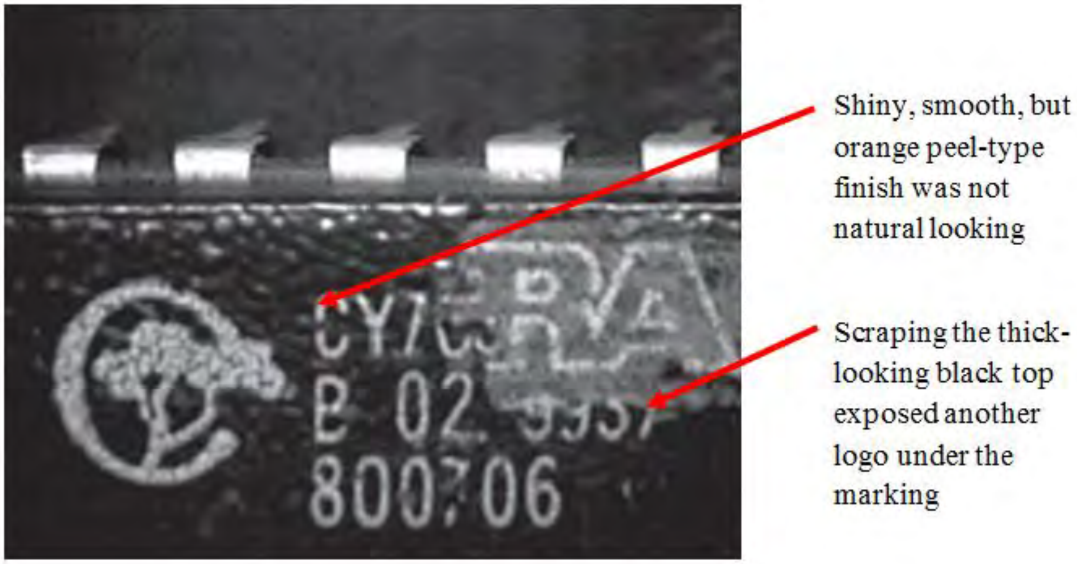

Shiny, smooth, but orange peel-type finish was not natural looking
Scraping the thick-looking black top exposed another logo under the marking

Figure 7. Blacktopping Example. This integrated circuit component was identified as counterfeit during visual inspection. The application of paint over the OCM‘s logo is an example of the blacktopping technique (from Government Accountability Office, 2010, p. 16).

The counterfeit market in China is big business, and affects the American bottom line in more ways than one. There is no effort to hide this practice in China; in fact, it is considered to be an acceptable business model in the Guangdong Province (Kirk, 2011). Further, counterfeit parts are often shipped from China to other nations that participate in the manufacture of legitimate components and subsystems; buying a system from an ally does not guarantee the pedigree of its parts (Kirk, 2011).

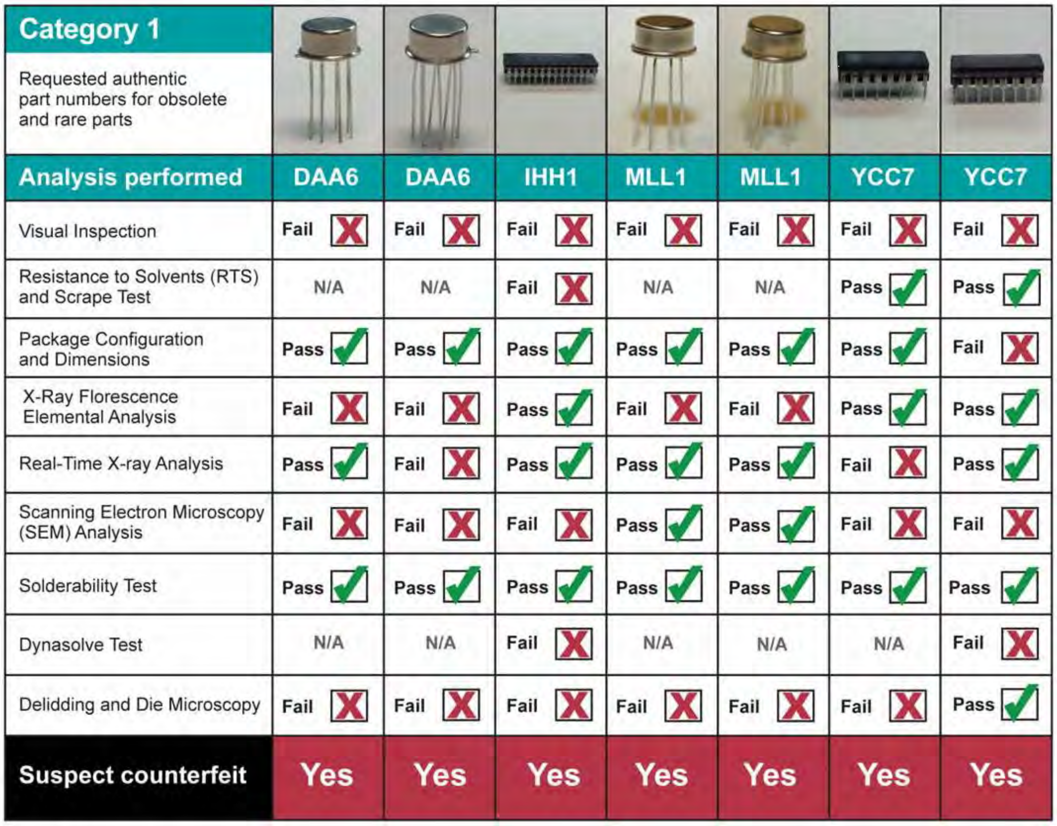
F. DETECTION

The parts ordered by DOD have distinct purposes, and have stated performance requirements documented in military specifications and standards. When counterfeit parts are put into a subsystem of a fighter jet, for example, they may work with little indication of a problem to the pilot; however, there may come a time when the old circuit cannot meet the demands of a modern weapons system. The circuit board that controls a subsystem within the plane (e.g., Global Positioning System (GPS), landing gear, targeting computer) may fail, causing anything from a minor annoyance to the pilot, to a potentially catastrophic full systematic shutdown or lockout.

Real life examples of this issue can be found in open United States government sources. One example from GAO Report 10–389 relates to Air Force GPS systems:

> Oscillators used for navigation on over 4,000 Air Force and Navy systems experienced a high failure rate and failed a retest. These oscillators were provided by a supplier that Global Positioning System engineers had previously disapproved as a supply source. Air Force officials stated that while the failure would not cause a safety-of-flight issue, it could prevent some unmanned systems from returning from their missions. (U.S. Government Accountability Office, 2010, p. 7)

There is no single test to determine if a part is counterfeit. As shown in Figure 8, the authentication process may pass one or two individual tests, but may still be found to be counterfeit.



Category 1

Requested authentic part numbers for obsolete and rare parts

Analysis performed	DAA6	DAA6	IHH1	MLL1	MLL1	YCC7	YCC7
Visual Inspection	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Fail ✗
Resistance to Solvents (RTS) and Scrape Test	N/A	N/A	Fail ✗	N/A	N/A	Pass ✓	Pass ✓
Package Configuration and Dimensions	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Fail ✗
X-Ray Florescence Elemental Analysis	Fail ✗	Fail ✗	Pass ✓	Fail ✗	Fail ✗	Pass ✓	Pass ✓
Real-Time X-ray Analysis	Pass ✓	Fail ✗	Pass ✓	Pass ✓	Pass ✓	Fail ✗	Pass ✓
Scanning Electron Microscopy (SEM) Analysis	Fail ✗	Fail ✗	Fail ✗	Pass ✓	Pass ✓	Fail ✗	Fail ✗
Solderability Test	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Pass ✓	Pass ✓
Dynasolve Test	N/A	N/A	Fail ✗	N/A	N/A	N/A	Fail ✗
Delidding and Die Microscopy	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Fail ✗	Pass ✓
Suspect counterfeit	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Figure 8. Comparison of Counterfeit Detection Techniques. DOD frequently orders rare and obsolete military grade components to support older in-service systems. This graphic shows a comparison of analysis techniques applied to seven requested authentic parts. All were found to be counterfeit (from Government Accountability Office, 2012, p. 6).

G. SUMMARY

The counterfeit parts problem is known, proven, and has been demonstrated operationally within DOD. The various studies and reports on this issue provide proposed steps to counteract the problem, but most represent a retroactive look at the dilemma of counterfeit parts. Counterfeiting is an ever changing marketplace, rendering the current control measures inadequate. This changing landscape was well illustrated by Raytheon‘s Vice President of Supply Chain Operations, as quoted in the 2012 SASC report:

> What keeps us up at night is the dynamic nature of this threat because by the time we‘ve figured out how to test for these counterfeits, they‘ve figured out how to get around it. And it‘s literally on almost a daily basis

> they change and the sophistication of the counterfeiting is amazing to us. We‘re finding that you have to go down to the microns to be able to figure out that it‘s actually a counterfeit. (U.S. Senate Committe on Armed Services, 2012, p. 7)

There is still no indication of how many illegitimate parts reside within operational systems, or on shelves at DOD warehouses.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INSUFFICIENCY OF CURRENT CONTROLS

A. NATIONAL DEFENSE AUTHORIZATION ACT

The counterfeiting control measures that have recently been proposed for DOD provide a strong starting point against this dynamic threat. The first of these is a 2012 amendment to the National Defense Authorization Act (NDAA) Section 818. This guidance provides broad solutions to detect and avoid counterfeit electronic parts in all stages of the acquisitions life cycle.

Within NDAA Section 818, the Secretary of Defense (SECDEF) is called upon to provide a department-wide definition of the terms ―counterfeit electronic part” and ―suspect counterfeit electronic part” (H.R. 1540, 2012). Until this mandate, there was no clear, legally binding definition of these terms, and each particular agency, group, or task force would provide their own definition depending on the specific circumstances of their investigation (H.R. 1540, 2012).

B. 2012 IMPLEMENTATION MEMORANDUM

Based on this requirement, the Acting Under Secretary of Defense for Acquisition, Technology, and Logistics (USD AT&L), Frank Kendall, provided guidance in a March 2012 memorandum, which acted as a broadcast identification of the problem, with mitigating steps that DOD agencies should follow in advance of the identification of counterfeit parts, as well as steps to be taken after the identification of a counterfeit part.

Kendall provided the following as his definition: ―For the purposes of this memorandum, counterfeit material is defined as ‗an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item‘s legally authorized source and has been misrepresented to be an authorized item of the legally authorized source'” (Kendall, 2012, p. 1).

This is a strong definition, but the NDAA focuses its emphasis on counterfeit electronic parts, whereas AT&L provides broader guidance that extends to other materiel. Specificity is lacking for certain circumstances, for example, when a previously authorized part becomes counterfeit. That is to say, when a computer that was once part of a DOD computing suite is sent off to be recycled, there is a risk that it will get into the hands of an illicit recycling operation. DOD must define the difference between a microprocessor that was once legitimate (and may still be legitimate for older platforms) and one that is straight counterfeit.

In addition to this, the NDAA Section 818 (b) (4) calls upon SECDEF to establish processes for ensuring that Department personnel issue reports in writing within 60 days of the identification of a possible counterfeit part incident. Additionally, this reporting should be done via the GIDEP or ―similar program designated by the secretary" (H.R. 1540, 2012).

The 2012 AT&L memo provides 10 points for department-wide action. Of those 10, point 7 calls out the GIDEP as the central reporting site: ―Ensure contractors and subcontractors reports of suspected or confirmed counterfeit items are entered into the Government-Industry Data Exchange Program (GIDEP) system, which will serve as the DOD central reporting repository" (Kendall, 2012, p. 1).

C. GIDEP INSUFFICIENCY

Though designated as the repository for all suspected counterfeit parts data, the GIDEP reports suspected counterfeit parts as ―Failure Experience Data" which prompts one of several types of reports: *Alerts, Safe-Alerts, Problem Advisories,* and *Agency Action Notices* (Government-Industry Data Exchange Program, 2009). These failure notices are received and disseminated to all GIDEP participants—several thousand in total—via the online GIDEP portal.

Some of these alerts may not be issued at all for two reasons. First, due to the sensitive nature of the end-user system information, some alerts must be redacted for classification prior to submission, which makes them of little or no value to the end user. Second, the supplier in question may be part of an ongoing investigation; if they are a GIDEP participant, then they will receive the alert, which will counteract the work of the investigators.

In most acquisition programs, prime contractors are contractually required to participate in the GIDEP program. However, self-reporting suspected counterfeit parts is the only way for a broader alert to be issued, and there is very little oversight to guide the levels of participation or reporting.

D. INDUSTRY CONTROLS

The NDAA Section 818 stipulates that contractors will not be subject to civil liability when they have made a reasonable effort to determine whether a counterfeit part was present. It is noteworthy that four years prior to enactment of 2012 NDAA, Grow, et al reflected the reluctance of contractors to use the GIDEP to report suspected counterfeits:

> [BAE‘s U.S. Division] has reported far more counterfeiting incidents than its rivals: 45 over the past three years. Industry executives say that large figure may reflect BAE‘s candor or its aggressive pursuit of low-priced chips from China. The Justice Department is investigating BAE‘s military electronic-parts procurement. This willingness to comply with reporting requirements could, in turn, cast doubt on the nature of a specific contractor‘s procurement practices when in fact, the problems are seen industry-wide. (Grow, Tschang, Edwards, & Burnsed, 2008, p. 2)

NDAA Section 818 (c)(3) requires DOD contractors to detect and avoid the use of counterfeit electronic parts and ―whenever possible" to obtain parts from original manufacturers or trusted suppliers. For parts that are hard to find or out of production, the trusted supplier is to notify DOD of the need to obtain the part from a source other than the authorized one. Upon receipt of the part, the prime contractor is to perform stronger verification testing through a DOD-approved testing program. There is no standard for implementation associated with this requirement (H.R. 1540, 2012).

Further, Section 818 (d) requires that the Department of Homeland Security (DHS) establish a risk-based methodology for the targeting of counterfeit electronic parts as they cross the border. This may alleviate some detection responsibility on the part of industry vendors who source parts from suppliers under DHS investigation H.R. 1540, 2012).

The NDAA falls short with Section 818 (e)(2)(A)(iii), where contractors are given specific guidance to establish policies and procedures that will ―abolish counterfeit parts proliferation.” This statement is far too broad to be of value (H.R. 1540, 2012).

Additionally, Section 818 (e)(2)(A)(v) mandates the use of mechanisms that enable the traceability of parts, but tracing the full pedigree of a part can be quite difficult (H.R. 1540, 2012). As noted by the SASC, each part could be sent through several different distributors before they reach an authorized one (U.S. Senate Committe on Armed Services, 2012). At that point, the part may be embedded within a functional sub-assembly. To test the part would require disassembly of the entire system, which in itself could destroy the electronic components.

While the NDAA and the AT&L memo are both very clear about the need to use covered contractors and trusted suppliers, there is a loophole that may still allow the independent distributor to operate. According to the Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association, the term ‗Covered Contractor‘ as pertains to Section 818 and the 2012 AT&L memo, refers to a contractor that is subject to the Cost Accounting Standard (CAS), thus leaving a threshold below which an independent supplier may be exempt:

> It is unclear whether acceptance of only one contract subject to CAS would render a contractor the kind of CAS-covered contractor that will be subject to these requirements. Applicability of these requirements to CAS covered contractors likely will cover all major defense contractors and will require these entities to flow down counterfeit avoidance and detection requirements to their subcontractors. Contractors that are not subject to CAS, such as commercial item contractors or small businesses, apparently would not fall within this ‗CAS-Covered Contractor‘ group. (American Bar Association Section Task Force on Counterfeit Parts, 2012, p. 15)

Therefore, the acquisition policies which favor small businesses would allow for a technical loophole from all pieces of the NDAA that pertain to counterfeit parts control. Either the NDAA should be amended to include all contractors and contract types, or the acquisitions policies should be updated to promote the strongest part pedigree instead of the lowest price, technically acceptable.

E. SUMMARY

The NDAA and AT&L memo both make a strong attempt to bound and quantify the problem, but the means to combat the problem are lacking. The GIDEP is an existing tool that is being re-purposed from its original 1986 MIL-STD to fit the current need. The use of GIDEP presents its own set of challenges including the ease and accountability of reporting suspected counterfeit parts.

According to the 2005 DSB report, ~~a~~ reexamination of economic models for producing low-volume products will require a joint government/industry program to develop new, more flexible factory technology capable of meeting both defense and commercial needs” (Defense Science Board, 2005, p. 4).

2012 control measures fail to provide the intended solution. Most of the reporting responsibility has been pushed to the contractor to verify a part‘s pedigree prior to end delivery, but there is no effort to provide a useful, joint, government and industry solution that provides real time guidance and alerts to this rapidly changing threat.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SOLUTION DEVELOPMENT

A. DESIGNED FAILURE

An immediate solution is required, as the DOD has already experienced the counterfeit parts problems from inexpensive non-conforming parts that accidentally find their way into the supply chain, to those parts that are specifically designed to infiltrate and undermine United States weapon systems.

The threat posed by failing parts is serious; as Lieutenant General Patrick O‘Reilly stated during his tenure as the Director of the Missile Defense Agency, ―We do not want a $12 million missile defense interceptor‘s reliability compromised by a $2 counterfeit part" (U.S. Senate Committe on Armed Services, 2012, p. i). More serious than the risk of a non-conforming part, is the threat found at the intersection of prolific inexpensive non-conforming microchips, and strategic placement of software within that microchip designed to fail at a particular point. The possibility of that threat was enhanced when chip-makers began to send offshore their operations in order to realize higher profits and increase supply. The 2005 DSB report identified this as a major vulnerability, and specifically noted the threat of having a Trojan horse program imbedded within the integrated circuits that are being included in United States Weapon Systems: ―such backdoor features could be used by an adversary to disrupt military systems at critical times" (Defense Science Board, 2005, p. 23). Additionally, when one considers the increasing interoperability and interconnectedness of intra-service platforms as well as cross-service weapon systems, the threat of a single virus affecting many users is amplified.

The implications of offshoring chip making are serious. The most telling quote can be found in the 2005 DSB report, which states the following:

> From a U.S. national security view, the potential effects of this restructuring are so perverse and far reaching and have such opportunities for mischief that, had the United States not significantly contributed to this migration, it would have been considered a major triumph of an adversary nation‘s strategy to undermine U.S. military capabilities. (Defense Science Board, 2005, p. 15)

Modern weaponry has a voracious appetite for integrated circuitry. Every platform contains several integrated circuits; an airplane, for example, has at least one circuit which controls the avionics computer, at least one that controls the heads-up display, and at least one that is specific to fire control (to name a few). An integrated circuit that fails will not cause the entire platform (airplane) to fail, but it will cause the particular subsystem which it controls to fail. The true threat is when an adversary knows parts are headed for a DOD system and places code within that circuit in order to cause a failure.

When contracting for electronic parts, if end-user information is passed along with the order, then it is relatively easy to deduce the types of software that can be used to interfere with the operation of the platform. For example, if contract information gets passed with the order which states Boeing is the end user, then the safe assumption would be that these chips are likely to end up in an airplane (either commercial or military), potentially interfering with the proper operation of that aircraft.

The enemy hacker potentially could embed a code within a batch of integrated circuits that targets the communications system. This code could be written such that the entire communications system would fail if a predetermined GPS coordinate is passed.

There is anecdotal evidence that suggests this might have already become a reality. A 2008 Institute of Electrical and Electronics Engineers (IEEE) article titled *The Hunt for the Kill Switch* tells the story of Israeli jets bombing a suspected nuclear installation within Syria (Adee, 2008, p. 1). According to Adee, the state-of-the-art Syrian radar did not pick up on the incoming strike. It is widely believed that the function of the radar had been blocked by a back-door code embedded within one of the radar chips during fabrication, and that this code caused the Syrian radar to cease functioning as the Israeli jets approached (Adee, 2008, p. 2).

Stronger than anecdotal evidence is the United States patent for an integrated circuit that has radio frequency code embedded within it. An excerpt from the patent abstract:

> An integrated circuit device is provided for attachment to a target. The integrated circuit is controllable to effect an action at the target, such as activating or deactivating the usefulness of the target. The integrated circuit has a logic and memory section connected to an antenna for receiving communications from an associated reader or scanner. The integrated circuit also has a component constructed to transition from a first state to a permanent second state. The integrated circuit also stores a hidden secret kill code, and upon receiving a matching kill code from the reader, permanently transitions the component to its second state. When the component is in the permanent second state, the integrated circuit is incapable of effecting the action on the target. The integrated circuit may also verify its function is disabled, and report a kill confirmation to the reader. (Atkinson & Conero, 2006, p. 1)

The United States has already seen the implications of malicious code on secure hardware devices. In 2008, a much publicized breach of DOD systems occurred wherein a foreign entity placed a simple piece of code on a flash drive which allowed a foreign security service to enter any system and read any file. That single piece of code on a single flash drive caused a massive data breach on both classified and unclassified networks; the cleanup effort was dubbed ―Operation Buckshot Yankee” and took approximately 14 months to complete. This moment was a wakeup call to the DOD and brought about the wider realization that the United States needed to take definitive action against this rapidly evolving cyber threat (Nakashima, 2010).

It was not until 2010 that the U.S. Cyber Command (USCYBERCOM) was made operational with the specific mission to conduct full spectrum military cyberspace operations (U.S. Cyber Command, 2014, para. 1). What is not clear, however, is the position that USCYBERCOM takes with regards to counterfeit hardware. Their focus is on information assurance and network reliability, but there is no obvious emphasis on bridging the gap between hardware pedigree and software reliability (U.S. Cyber Command, 2014, para. 4).

One mitigation strategy has been implemented via the Defense Microelectronics Activity (DMEA). DMEA has initiated a trusted foundry program, which is designed to provide uninterrupted access to the microprocessors that are used by the United States Military. This is accomplished by identifying foundry partners that are reliable, and have been vetted through the DMEA trusted foundry criteria (Defense Microelectronics Activity Trusted Foundry Program, 2014).

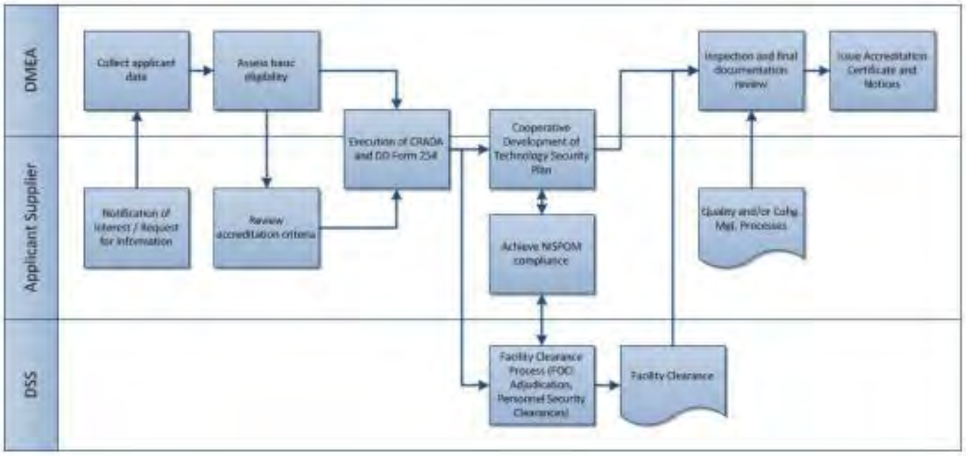

DMEA
Applicant Supplier
DSS
Collect applicant data
Assess basic eligibility
Notification of Interest / Request for Information
Review accreditation criteria
Execution of CRADA and DD Form 254
Cooperative Development of Technology Security Plan
Achieve NISPOM compliance
Facility Clearance Process (FOC) Adjudication, Personnel Security Clearances)
Facility Clearance
Inspection and final documentation review
Issue Accreditation Certificate and Notices
Quality and/or Cofig. Mgt. Processes

Figure 9. Trusted Supplier Accreditation Process. This describes the DMEA Trusted Supplier Accreditation Process. There is no obvious verification or reevaluation process after certification is achieved (from Defense Microelectronics Activity, 2014).

Ideally, once a supplier is passed through this trusted foundry program, they will provide microprocessors that do not require heavy validation and invasive testing to determine part pedigree. The assumption is that a trusted foundry, especially one within the United States, will not produce parts that are harmful to the United States. However, this does not prevent a malefactor, insider threat, or disgruntled employee from creating a code and embedding it within a chip.

From the hardware perspective, the NDAA Section 818 is designed to identify counterfeits at multiple contractor levels, after delivery has been accepted by the prime contractor, and ideally before delivery is made to the Government. However, due to a variety of factors, only a fraction of these parts are identified, and of those identified parts, only a fraction can be traced back to their source. Identification of the counterfeit often comes after the part is already embedded within the platform, which causes extra time and cost to disassemble, repair, and reassemble.

With regard to software, the testing required to verify a circuit is free from illicit code is extremely time-consuming, and when considering an order size of several thousand chips, it is both time and cost prohibitive. As noted by the 2007 DSB report titled *Mission Impact of Foreign Influence on DOD Software*,

> The problem of detecting vulnerabilities is deeply complex, and there is no silver bullet on the horizon. Once malicious code has been implanted by a capable adversary, it is unlikely to be detected by subsequent testing…. Current tools find about one third of the bugs prior to deployment that are ever found subsequently, and the rate of false positives is about equal to that of true positives. (Defense Science Board, 2007, p. ix)

The problem of counterfeit parts is highly dynamic, yet the solutions proposed by Government entities are somewhat static. As noted earlier, the sophistication of the counterfeiters varies greatly and their tactics change often.

The United States is behind the threat curve where this hardware to software crossroads occurs, as noted by the 2007 DSB report:

> From a defensive perspective, microelectronics and its associated software cannot be separated. While the offense may be able to attack either and meet operational objectives, the defense must be prepared for the offense to attack at the seam of the software and hardware. If this offensive approach is done well and the defense examines the software and hardware only as independent elements, the offense is likely to go unnoticed until too late. (Defense Science Board, 2007, p. 4)

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

Launching the Defense Acquisition Reform Initiative in 1997, SECDEF Cohen accelerated the move to Commercial-Off-The-Shelf (COTS) technology, which provided better capabilities to the warfighter, at a faster pace, and with less cost to the taxpayer. While all of these benefits were realized in one way or another, product integration and parts obsolescence became increasingly problematic. Technology development in the commercial sector far outpaced the DOD‘s ability to react, and parts that were required for COTS-based systems became harder to acquire.

Manufacturing was moved off-shore in order to capitalize on favorable market conditions, low labor costs, and low market entry costs. According to the 2005 DSB Report:

> Pressure on U.S. IC suppliers for high return on invested capital has compelled them to outsource capital intensive manufacturing operations. Thus, the past decade has seen an accelerating trend towards vertical disaggregation in the semiconductor business. Companies whose manufacturing operations once encompassed the full range of integrated circuit activities from product definition to design and process development, to mask-making and chip fabrication, to assembly and final test and customer support, even materials and production equipment, are contracting out nearly all these essential activities. (Defense Science Board, 2005, p. 4)

This outsourcing, while extremely dangerous to the integrity of the United States microchip supply, is a natural outgrowth of globalization. Rather than trying to reverse the inevitable tide of continued globalization, the United States government needs to be intelligent about how the acquisition of electronics is managed.

Ultimately, the problem of counterfeit parts in the DOD supply line is an issue of parts obsolescence. According to the Defense Microelectronics Activity (DMEA) director in 2008, ―The defense community is critically reliant on a technology that obsoletes itself every 18 months, (and) is made in unsecure locations over which we have absolutely no market share or influence" (Gillies, 2008, p. 1).

The steps being undertaken by DOD and Congress shift the responsibility for microelectronic parts pedigree to the contractor as the supplier of the electronic parts; but this policy does not address the continued need for DOD to acquire parts that are unavailable, obsolete, or otherwise hard to find.

Parts obsolescence is inevitable in the modern military, but the means to deal with parts obsolescence can be found in the early phases of development. If consideration is given to life cycle management and technology refresh, then future problems can be mitigated, thus elongating the total life cycle of the system being developed.

VI. RECOMMENDATIONS

A. SUMMARY

Statutory measures designed to stem the flow of counterfeit electronic parts into the DOD supply chain are not effective at curbing the threat, which evolves more rapidly than both our controls, and the systems into which these threats are introduced. Current counterfeit parts control measures are designed to identify counterfeit parts after they have reached the customer, rather than closing the holes in the supply chain. Existing policy is inadequate in addressing the underlying economic, technological, and implementation issues that underpin the counterfeit parts problem. A joint government and industry approach is required in order to more effectively control this issue and ensure the quality and authenticity of electronic parts. Additionally, DOD should more consistently apply the system acquisition framework in ways that aid in the identification and accommodation of obsolescence, refresh, and service life extension concerns. Recommended areas for further investigation and potential strategies for mitigating the threat are identified below.

B. AREAS FOR FURTHER STUDY

- **Greater government oversight through the development of a new agency**:

The National Institute of Standards and Technology (NIST), a subordinate agency of the Department of Commerce, does provide guidance and suggestions on supply chain risk management and the identification of counterfeit electronic parts; however, there is no overriding government agency that is wholly dedicated to supply chain risk management and counterfeit parts mitigation.

The solutions outlined in the conclusions above all touch on a piece of the counterfeit parts problem, but they are disjointed and do not represent an integrated effort to combat a problem that has been steadily growing over time. The primary tracking system for counterfeits, GIDEP, is a system that was created for another purpose, and is being used for lack of an appreciable alternative.

A government agency or service, perhaps an element of the Department of Commerce, could set acceptance standards, consolidate tracking and monitoring efforts, and strive to adequately keep ahead of this highly dynamic problem. If correctly implemented and supported, such a service would have the resources and authority to concentrate its efforts on the latest counterfeiting techniques, and could provide real-time counterfeiting threat data through a variety of sources, which, if classified, would help to prevent compromise of any ongoing investigations. This service could also provide a database, whose sole purpose is the reliable conveyance of information pertaining to counterfeit parts.

A 2010 GAO Report noted the lack of government oversight, policy, or processes to prevent counterfeit parts. Also noted in that report was the fact that the DOD is limited in their ability to fully scope the problem (U.S. Government Accountability Office, 2010). As of 2010, the Defense Logistics Agency (DLA), which supplies the DOD with most of its spare parts, neither consistently reported nor maintained a list of instances where counterfeit parts were found. A dedicated agency would provide the much needed oversight and verification of industry‘s compliance with statutory measures. Such an organization could provide authentication and validation of sites that have been accredited through the DMEA process, and would identify solutions to keep critical electronics flowing to the military.

The drawback of this solution would be the requirements that are imposed upon a government entity. Reports to Congress, requests for information, and other high level products that are required by a government entity will all mire this agency in administrative requirements, which will reduce their effectiveness and ability to quickly react to threats. Additionally, due to freedom of information act requests, it is possible that their active investigations could become public, thereby reducing their effectiveness.

- **Greater collaboration with industry**

The solutions provided by the government put the bulk of the reporting responsibility on the contractor. This is a fundamental flaw; industry has a similar vested interest in the identification and prevention of counterfeit electronics as government. The reputation of the contractor, in addition to the possible negative reaction of shareholders all affects the bottom line of a company that provides electronic parts to the government.

It is incumbent upon the government to work collaboratively with industry, vice antagonistically. Traditionally, industry is quicker to identify problems in their supply lines, and more agile in the implementation of solutions. Given that, industry has been dealing with counterfeit parts for years and has devised and implemented solutions to protect its supply chain. United States companies may design technology domestically but outsource production overseas, while maintaining strict performance standards for their products.

Industry has already made solutions that bridge the hardware/software gap as well. According to an EDN Network article titled *Advanced Security Prevents Counterfeit Products*, industry is already using asymmetric cryptography, the core technology behind digital signatures, to secure online transactions and ensure confirmation of product originality. When a printer, for example, leaves the assembly line, it is given a particular radio frequency identification (RFID). Upon the use of that printer, the RFID is checked to ensure it is a valid platform, and will not work if the RFID is not confirmed to be valid (Richetto, 2011).

Greater collaboration with industry would also help with one of the primary drivers of counterfeit electronics, the electronic recycling market. At the end of a product life cycle, the device or platform cannot simply be shipped off to an unseen entity; the government should be working together with industry to identify solutions to life cycle management issues. Establishing a strong electronics recycling industry in the United States could be profitable for industry, and beneficial for government.

- **Counterfeit parts controls in the system acquisition process**

Technology refresh (TR), is defined as ―the periodic replacement of both custom-built and COTS system components, within a larger DOD weapon system, to assure continued supportability throughout its life cycle (Defense Acquisition University, 2014)." Rather than employing a full DOD 5000 series acquisition for technology refresh (TR), system requirements must be structured dynamically, to accommodate capability insertion needs within existing weapon systems throughout their service life. The framework for this begins in the early stages of system development. DOD must apply considerations for counterfeit parts controls as early as possible in system requirements, specifically in draft Capabilities Development Document (CDD) development during the Materiel Solution Analysis phase of system acquisition. When writing system hardware requirements, consideration should be given to the backwards compatibility that will be required for integrated circuits and discrete electronics. Much of the counterfeit parts problem can be traced to a product life cycle that has been extended well beyond its anticipated service life, especially when there has been no consideration given to TR. This should also be considered during development of the system‘s Life-Cycle Sustainment Plan, which should include standard considerations for TR.

Ideally, each weapon system will have a significantly increased service life by providing new technology insertions. When performed correctly, TR ensures long term weapon system availability, and reduces the impacts of diminishing manufacturing sources (Defense Acquisition University, 2014). However, there is no specific DOD policy on how to structure a TR program; therefore, each element of the DOD is applying this differently based on their specific requirements. The CDD and Life-Cycle Sustainment Plan are tools that can aid in the consistent application of counterfeit parts controls across dissimilar programs of record.

LIST OF REFERENCES

Adee, S. (2008). *The hunt for the kill switch.* Institute of Electrical and Electronic Engineers (IEEE) Spectrum. Retrieved 2013, from http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

American Bar Association Section Task Force on Counterfeit Parts. (2012). *A white paper regarding Department of Defense implementation of section 818 of the NDAA for 2012.* Chicago, IL: American Bar Association. Retrieved 2014, from http://www.americanbar.org/content/dam/aba/administrative/public_contract_law/aba_pcl_taskforce_on_counterfeit_part_white_paper.authcheckdam.pdf

Atkinson, P., & Conero, R. (2006). *U.S. Patent No. WO2007008916 A3.* Washington, DC: U.S. Patent and Trademark Office.

Defense Acquisition University. (2014). 3.5.3 Technology Refresh. Retrieved 2014, from https://acc.dau.mil/CommunityBrowser.aspx?id=495014

Defense Microelectronics Activity. (n.d.). Trusted Foundry Program. Retrieved 2014, from http://www.dmea.osd.mil/trustedic.html

Defense Science Board. (1992). *Report of task force on microelectronics research facilities.* Washington, DC: U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics. Retrieved 2013, from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA274529

Defense Science Board. (2005). *Report of task force on high performance microchip supply.* Washington, DC: U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics. Retrieved 2013, from http://www.acq.osd.mil/dsb/reports/ADA435563.pdf

Defense Science Board. (2007). *Report of task force on mission impact of foreign influence on DOD software.* Washington, DC: U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics. Retrieved 2013, from http://www.acq.osd.mil/dsb/reports/ADA486949.pdf

Gillies, A. (2008). Pentagon worries about chinese chips. *Forbes*. Retrieved 2015, from http://www.forbes.com/2008/09/04/pentagon-defense-contractors-biz-wash-cz_atg_0904beltway.html

Government Accountability Office. (2010). *Defense supplier base: DOD should leverage ongoing initiatives in developing its program to mitigate risk of counterfeit parts* (GAO 10–389). Washington, DC: Government Accountability Office. Retrieved 2013, from http://www.gao.gov/new.items/d10389.pdf

Government Accountability Office. (2012). *Suspect counterfeit electronic parts can be found on internet purchasing platforms* (GAO 12-375*).* Washington, DC: Government Accountability Office. Retrieved 2014, from http://gao.gov/assets/590/588736.pdf

Government-Industry Data Exchange Program. (2009). *GIDEP operations manual, chapter 7: failure experience data*. Retrieved 2014, from http://www.gidep.org/about/opmanual/opmanual.htm

Government-Industry Data Exchange Program (GIDEP) home page [web site]. (2015). Retrieved 2015, from http://www.gidep.org/

Grow, B., Tschang, C., Edwards, C., & Burnsed, B. (2008). Dangerous fakes. *Bloomberg Business*. Retrieved 2014, from http://www.bloomberg.com/bw/stories/2008-10-01/dangerous-fakes

Historic computer images. (2013). Retrieved 2013, from http://ftp.arl.army.mil/ftp/historic-computers/

How microprocessors work. (2013). Retrieved 2013, from http://computer.howstuffworks.com/microprocessor.htm

Kendall, F. (2012). *Overarching DOD counterfeit prevention guidance.* Washington, DC: U.S. Department of Defense, Under Secretary of Defense for Acquisition, Technology, and Logistics. Retrieved 2014, from http://www.acq.osd.mil/log/sci/anti-counterfeit/Counterfeit-Prevention-Guidance.pdf

Kirk, R. (2011). *2011 special 301 report.* Washington, DC: United States Trade Representative. Retrieved 2014, from https://ustr.gov/sites/default/files/uploads/gsp/speeches/reports/2011/301/2011%20Special%20301%20Report.pdf

Nakashima, E. (2010, August 24). Defense official discloses cyberattack. *Washington Post*. Retrieved 2014, from http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html

National Academy of Engineering, Committee on the Offshoring of Engineering. (2008). *The offshoring of engineering: facts, unknowns, and potential implications.* Washington, DC: National Academies Press. Retrieved 2013, from http://pcic.merage.uci.edu/papers/2008/OffshoringofEngineering.pdf

National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Cong. (2012)

Nobel Prize. (2014). *The history of the integrated circuit*. Retrieved 2014, from http://www.nobelprize.org/educational/physics/integrated_circuit/history/

Richetto, D. (2011, November 4). *Advanced security prevents counterfeit producs*. Retrieved 2014, from http://www.edn.com/design/consumer/4368557/Advanced-security-prevents-counterfeit-products

Rochester Electronics. (2011). *The cost of counterfeit semiconductors to the electronics industry.* Newburyport, MA: Rochester Electronics. Retrieved 2013, from https://www.rocelec.com/media/uploads/documents/Cost_of_Counterfeit_Semiconductors_Jun_8_11.pdf

Rumberg, P. (2013, December). USS Missouri fire control computer photo [Image]. Retrieved 2014, from photographer.

U.S. Cyber Command. (2014). Retrieved 2014, from http://www.stratcom.mil/factsheets/2/Cyber_Command/

U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation. (2010). *Defense industrial base assessment: counterfeit electronics.* Washington, DC: U.S. Department of Commerce. Retrieved 2014, from https://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010

U.S. Department of Defense. (1986). *Government/Industry Data Exchange Program (GIDEP) Contractor Participation Requirements (MIL-STD-1556B).* Washington, DC: U.S. Department of Defense. Retrieved 2013, from http://everyspec.com/MIL-STD/MIL-STD-1500-1599/MIL_STD_1556B_1350/

U.S. Department of Defense. (1996). *Notice of Cancellation, MIL-STD-1556B, Notice 1.* Washington, DC: U.S. Department of Defense. Retrieved 2013, from http://docimages.assistdocs.com/watermarker/transient/BF68D4CBBBCF403FB618A75E771F1813.pdf

U.S. Senate Committee on Armed Services. (2012). *Inquiry into counterfeit electronic parts in the Department of Defense supply chain (Report 122-167).* Washington, DC: United States Senate. Retrieved 2014, from http://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

Villasenor, J., & Tehranipoor, M. (2013). *The hidden dangers of chop-shop electronics: clever counterfeiters sell old components as new, threatening both military and commercial systems.* Institute of Electrical and Electronic Engineers (IEEE) Spectrum. Retrieved 2014, from http://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California